

## MÉTHODE DE GESTION DE LA SÉCURITÉ D'APPLICATIONS AVEC UN MODULE DE SÉCURITÉ.

La présente invention concerne le domaine des réseaux mobiles appelés aussi réseaux cellulaires. Elle concerne plus particulièrement la gestion de la sécurité des applications mises en œuvre avec un module de sécurité associé à un équipement mobile de téléphonie mobile.

- Le module de sécurité d'un téléphone mobile ou portable est connu sous l'appellation "carte SIM" (Subscriber Identity Module) constituant l'élément central de la sécurité de ces téléphones. L'opérateur de téléphonie introduit, à la fabrication et/ou lors d'une phase de personnalisation, un numéro appelé IMSI (International Mobile Subscriber Identification) servant à identifier d'une manière sûre et unique chaque abonné désirant se connecter sur un réseau mobile. Chaque téléphone mobile, appelé équipement mobile ci-après, est identifié physiquement par un numéro stocké dans une mémoire non volatile de l'équipement mobile. Ce numéro, appelé IMEI, (International Mobile Equipment Identifier) contient une identification du type d'équipement mobile et un numéro de série servant à identifier de manière unique un équipement mobile donné sur un réseau du type GSM (Global System for Mobile communications), GPRS (General Packet Radio System) ou UMTS (Universal Mobile Telecommunications System). De plus, un équipement mobile est caractérisé par une version de logiciel SVN (Software Version Number) indiquant l'état de mise à jour du logiciel de base installé sur l'équipement mobile. La combinaison de l'identification du type et du numéro de série de l'équipement mobile avec la version de logiciel (SVN) donne une nouvelle identification, appelée IMEISV (International Mobile Equipment Identifier and Software Version Number).
- Le même concept d'identification s'applique également au WLAN (Wireless LAN) ou au câble TV bidirectionnel. L'identifiant physique peut être une adresse MAC (Media Access Control) qui correspond à l'adresse unique identifiant la configuration du matériel d'un utilisateur sur un réseau IP (Internet Protocol) et la version de logiciel peut être transmise par des protocoles de couche supérieure basés sur IP.
- Les normes ETSI ("European Telecommunications Standards Institute"), définissent une station mobile (MS, mobile station) composée d'un équipement mobile (ME,

- 2 -

mobile equipment) et d'un module d'abonné (SIM, subscriber identity module). Ce module d'abonné est en général amovible c'est-à-dire qu'il peut être soit retiré soit transféré d'un équipement mobile à un autre.

Lors de la mise en service d'un équipement mobile, plus particulièrement lors de sa 5 connexion au réseau d'un opérateur, des informations comprenant les données d'identification sont échangées entre l'équipement mobile et le centre de gestion de l'opérateur qui autorise ou non son utilisation.

Le document EP0757502 décrit une méthode de verrouillage d'un module d'identification d'utilisateur lorsque l'identificateur physique de l'équipement mobile 10 IMEI se trouve sur une liste noire. Lorsque l'équipement mobile se connecte au réseau mobile, il transmet l'identificateur IMEI à un centre de gestion. Ce dernier vérifie par comparaison l'identificateur reçu avec le contenu d'une base de donnée où l'opérateur enregistre les identificateurs d'équipements mobiles volés ou défectueux. Si un identificateur reçu est présent dans cette base de données, le 15 centre de gestion transmet un message contenant une commande de blocage à l'équipement mobile concerné. Cette commande, après vérification de son authenticité, est transmise au module d'identification qui exécute une procédure de verrouillage empêchant toute connexion ultérieure de l'équipement mobile au réseau.

20 Le document US5864757 décrit une méthode d'activation d'un combiné mobile avec un module d'abonné basée sur l'utilisation d'une clé propre au combiné produisant un code correspondant à un identifiant du module d'abonné. Le combiné inclut une clé unique inviolable. Lors de son activation, le centre de gestion de l'opérateur transmet un message au combiné servant à calculer une clé spécifique à l'opérateur 25 en utilisant la clé unique du combiné. Cette nouvelle clé est utilisée en combinaison avec un identificateur du réseau ou du module d'abonné pour générer un mot de contrôle qui est confronté avec un code stocké dans le module d'abonné. Si le mot de contrôle concorde avec le code du module d'abonné, le combiné est activé.

Les méthodes décrites dans ces deux documents traitent exclusivement d'aspects 30 nécessitant une identification physique de l'équipement mobile basée par exemple

sur l'identificateur IMEI. Lorsque ces méthodes sont mises en œuvre, leurs effets se concentrent uniquement sur le blocage / déblocage du module d'abonné et/ou de l'équipement mobile de manière à empêcher toute connexion de l'équipement mobile au réseau.

- 5 Actuellement un équipement mobile offre à l'utilisateur, en plus de sa fonction usuelle d'établissement de conversations téléphoniques par le biais d'un accès à un réseau mobile, l'utilisation de nombreux autres services supplémentaires à valeur ajoutée tels que la consultation de diverses informations, les opérations bancaires à distance, le commerce électronique, l'accès à du contenu multimédia, etc. Ces  
10 services évolués nécessitent un niveau de sécurité de plus en plus élevé afin de prémunir les utilisateurs contre les fraudes éventuelles causées par des tiers cherchant à exploiter des failles de sécurité qui peuvent apparaître sur les équipements mobiles.

Une vérification devient donc nécessaire au moins à deux niveaux: d'une part au  
15 niveau de l'équipement mobile lui-même et d'autre part à celui des applications logicielles permettant le fonctionnement des différents services proposés par l'opérateur ou par des parties tierces. Il s'agit de garantir que le module d'abonné fonctionne seulement avec un équipement mobile de type et de version de logiciel dûment autorisé ou homologué par l'opérateur et/ou par les fournisseurs  
20 d'applications. Par fonctionnement du module d'abonné, on entend sa capacité de permettre l'utilisation de services sollicités par un utilisateur en exécutant un certain nombre d'applications logicielles préalablement installées dans une mémoire de l'équipement mobile et qui se servent du module d'abonné comme moyen de protection.

- 25 Ces applications exécutées dans l'équipement mobile utilisent des ressources disponibles dans le module d'abonné. Par ressources, on entend diverses fonctions et données nécessaires au bon fonctionnement d'une application. Certaines de ces ressources peuvent être communes à plusieurs applications, notamment les fonctions liées à la sécurité. Le module d'abonné peut ainsi bloquer ou altérer le  
30 fonctionnement de certaines applications pour lesquelles les conditions de sécurité établies par l'opérateur et/ou les fournisseurs d'applications ne sont pas respectées

- 4 -

dans l'équipement mobile en question ou les droits de l'utilisateur de l'équipement mobile sont insuffisants.

Les documents cités ci-dessus ne couvrent pas les aspects logiques relatifs à un ensemble d'équipements mobiles comme par exemple des informations relatives à  
5 des applications logicielles installées, un numéro de version de logiciel ou encore une référence de type ou de modèle de l'équipement mobile, etc. Il s'agit donc de disposer d'une méthode de gestion ciblée des ressources du module d'abonné afin d'activer / désactiver d'une manière sélective des applications ou des fonctions d'applications utilisant ces ressources. Il n'est toutefois pas souhaitable que ces  
10 opérations empêchent l'équipement mobile d'accéder au réseau en bloquant totalement le module d'abonné.

Le but de la présente invention est de proposer une méthode de gestion de la sécurité de l'ensemble équipement mobile, module d'abonné, applications afin de limiter les risques liés au fait qu'un module d'abonné soit utilisé à mauvais escient  
15 par des applications exécutées sur un équipement mobile de type et/ou de version de logiciel ne remplissant pas certains critères de sécurité préétablis.

Un autre but est de protéger l'utilisateur de l'équipement mobile ainsi que les fournisseurs d'applications concernés contre les abus résultants d'un clonage de l'équipement mobile et/ou du module d'abonné.

20 Ces buts sont atteints par une méthode de gestion de la sécurité d'applications fonctionnant dans un équipement connecté à un réseau, ledit réseau étant administré par un serveur de contrôle d'un opérateur, lesdites applications utilisant des ressources (données ou fonctions) stockées dans un module de sécurité relié localement audit équipement, comprenant les étapes préliminaires suivantes:  
25 • réception de données comprenant au moins le type et la version de logiciel de l'équipement et l'identité du module de sécurité, via le réseau, par le serveur de contrôle,  
• analyse et vérification par le serveur de contrôle desdites données,

- 5 -

- génération d'un cryptogramme à partir du résultat de la vérification sur lesdites données, et transmission dudit cryptogramme, via le réseau et l'équipement, au module de sécurité,

ladite méthode est caractérisée en ce que le module de sécurité analyse le

5 cryptogramme reçu et active, respectivement désactive des ressources (données ou fonctions) utilisées par au moins une application installée dans l'équipement, ledit cryptogramme comprenant des instructions conditionnant le fonctionnement de l'application selon des critères préétablis par le fournisseur de ladite application et/ou l'opérateur et/ou l'utilisateur de l'équipement.

10 Les ressources du module d'abonné sont bloquées de manière ciblée, ceci dans le but de bloquer ou réduire la fonction de certaines applications. On ne bloque pas directement des applications de l'équipement: on agit de manière indirecte sur les applications, c'est-à-dire que l'effet de blocage va se manifester uniquement lorsque l'équipement essaiera d'exécuter ces applications.

15 Cette méthode s'applique de préférence au réseau mobile. Par conséquent, l'équipement est un équipement mobile, comme par exemple un équipement de téléphonie mobile ou téléphone portable. Le module de sécurité est un module d'abonné inséré dans le téléphone portable du type carte SIM (subscriber identity module). Cet ensemble se connecte à un réseau mobile du type GSM (Global

20 System for Mobile communications), GPRS (General Packet Radio System), UMTS (Universal Mobile Telecommunications System) ou autre, géré par un serveur de contrôle d'un opérateur. Des applications logicielles sont installées dans l'équipement mobile et configurées de manière à utiliser des ressources (données ou fonctions) présentes dans le module d'abonné. Elles ne peuvent donc être  
25 utilisées dans leur intégrité seulement si les conditions de sécurité sont satisfaites selon des critères préétablis par l'opérateur et/ou le fournisseur d'applications. Cette vérification des critères est à la charge du serveur de contrôle. L'application, suite aux instructions envoyées par le serveur de contrôle, est finalement à la charge du module de sécurité qui peut laisser libre ou bloquer l'accès à des ressources  
30 nécessaires au bon fonctionnement d'une application installée dans l'équipement mobile.

- 6 -

Les données de ces ressources peuvent comprendre des informations tels que numéro de comptes, des programmes (sous forme de code pouvant être installé dans l'équipement mobile), des clés d'encryption/décryption, des droits d'accès à du contenu, etc.

- 5 Les fonctions de ces ressources peuvent comprendre des algorithmes cryptographiques, des processus de vérification, des processus de génération de signatures digitales, des processus d'encryptage, des processus d'authentification, des processus de validation de données, des processus de contrôle d'accès, des processus de sauvegarde de données, des processus de paiement etc.
- 10 Le serveur de contrôle joue un rôle essentiel en gérant les éléments de confiance ou de sécurité liés à l'ensemble équipement mobile / module abonné. Il interprète les données qui lui sont transmises par l'équipement mobile afin de contrôler ou limiter l'utilisation d'applications, fonctions ou ressources disponibles au moyen du module d'abonné.
- 15 Le serveur recevant les informations d'identité d'un équipement mobile et de son module d'abonné et comprenant l'IMEISV et l'IMSI décide, selon certains critères, si une nouvelle instruction doit être envoyée au module d'abonné pour redéfinir un nouveau profil de protection définissant les ressources du module d'abonné pouvant être utilisées par les applications exécutées dans l'équipement mobile. Les critères 20 peuvent se référer, par exemple, à la mise à jour de la version de logiciel installée sur l'équipement mobile, au téléchargement de nouvelles applications sur l'équipement mobile, à la période de mise à jour du profil de protection, au nombre de connexions au réseau, à la technologie utilisée pour l'accès au réseau, à l'identité du réseau d'accès utilisé. Ils sont également liés à différents risques 25 associés au matériel ou aux logiciels utilisés que l'opérateur et/ou le fournisseur d'applications et/ou l'utilisateur de l'équipement mobile désirent prendre en compte.

La méthode selon l'invention s'exécute généralement lors de chaque connexion de l'équipement mobile au réseau ou après chaque mise à jour de la version de logiciel de l'équipement mobile ou de celle du module d'abonné ou encore de celle de

- 7 -

ressources sur le module d'abonné. Elle peut également être exécutée lors de chaque activation ou désactivation d'une application sur l'équipement mobile.

Selon une variante, elle peut être exécutée périodiquement à un rythme donné par le serveur de contrôle ou après chaque démarrage d'une application sur 5 l'équipement mobile. Selon une autre variante, le module d'abonné ne va pas recevoir un nouveau message du centre de contrôle tant que l'identifiant IMEISV de l'équipement mobile demeure inchangé.

Lors de la ré-initialisation du module d'abonné, il est préférable de bloquer un certain nombre de ressources jusqu'à l'arrivée du cryptogramme. Ainsi, si 10 l'équipement mobile veut intercepter le cryptogramme et ne pas le transmettre au module abonné, tout ou partie des ressources (données ou fonctions) du module d'abonné ne seront pas disponibles pour les applications exécutées dans l'équipement mobile. Selon le type de réalisation, il est possible que certaines 15 ressources du module d'abonné utilisées par des applications d'un bas niveau de sécurité, soient mises en fonction par défaut avant l'arrivée du cryptogramme. Ceci est également le cas pour des ressources nécessaires à l'obtention de l'accès au réseau, sans quoi l'envoi du cryptogramme ne serait pas possible par ce même réseau.

Lorsque le module d'abonné vérifie la validité du cryptogramme, il identifie aussi de 20 manière indirecte l'équipement mobile et s'assure que les données viennent effectivement du serveur de contrôle. Autrement dit, par ce cryptogramme, le serveur de contrôle donne implicitement l'assurance au module d'abonné que le type et la version de logiciel de l'équipement mobile ont été pris en compte avant de 25 transmettre des instructions au module abonné. Ces dernières sont, de ce fait, chargées, le cas échéant, de donner ou refuser l'autorisation d'utilisation complète ou partielle de certaines applications de l'équipement mobile.

L'équipement mobile joue un rôle de relais dans cette étape de vérification en établissant un dialogue quasi direct entre le module d'abonné et le serveur de contrôle. Ainsi la sécurité des messages échangés est assurée de bout en bout 30 entre le serveur de contrôle et le module d'abonné via l'environnement d'exécution

- 8 -

des applications mises en œuvre sur l'équipement mobile. Celui-ci ne peut donc pas "tricher" ou transformer les données vis-à-vis du module d'abonné.

La présente invention concerne également un module de sécurité comprenant des ressources destinées à être localement accédées par au moins une application

- 5 installée dans un équipement relié à un réseau, ledit équipement comprenant des moyens de lecture et de transmission de données comprenant au moins le type et la version de logiciel de l'équipement et l'identifiant du module de sécurité, ledit module étant caractérisé en ce qu'il comprend des moyens de réception, d'analyse et d'exécution d'instructions contenues dans un cryptogramme lesdites instructions
- 10 conditionnant le fonctionnement de l'application selon des critères préétablis par le fournisseur de ladite application et/ou l'opérateur et/ou l'utilisateur de l'équipement.

Ce module de sécurité est utilisé par exemple comme module d'abonné ou carte SIM connecté à un équipement mobile.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux figures annexées données à titre d'exemple nullement limitatif, à savoir:

- La figure 1 illustre un schéma bloc montrant les différentes parties de l'équipement mobile et du serveur mises à contribution lors de l'échange des données d'identification et du cryptogramme.
- 20 - La figure 2 représente un schéma bloc de l'ensemble équipement mobile / module abonné avec les interactions entre les différentes parties lors du fonctionnement d'une application.

La figure 1 montre l'ensemble équipement mobile (CB) et module d'abonné (SIM) qui transmet via un réseau mobile (NET) des données d'identification (ID) que le serveur de contrôle (CSE) vérifie. Ce dernier renvoie un cryptogramme (J) vers le module d'abonné via l'équipement mobile (CB). L'équipement mobile (CB) inclut une ou plusieurs applications logicielles (APP) fonctionnant dans un environnement d'exécution (AEE). Ces applications proviennent soit d'un fournisseur d'applications

- 9 -

(FA) associé au serveur de contrôle (CSE) de l'opérateur, soit, elles sont programmées d'origine par le fabricant de l'équipement mobile.

Le module d'abonné inclut des ressources (RES) utilisées par les applications logicielles (APP).

- 5 La figure 2 montre que le fonctionnement des applications (APP) de l'équipement mobile (CB) dépend directement des ressources (RES) disponibles dans le module d'abonné. En l'absence de ressources adéquates, l'application peut, soit ne pas démarrer, soit fonctionner de façon très limitée avec des paramètres par défaut pouvant générer des messages d'erreur invitant l'utilisateur à accomplir des actions correctives nécessaires comme par exemple changer d'équipement mobile (CB) ou 10 de module d'abonné (SIM).

L'équipement mobile (CB) s'identifie, par exemple lors de chaque requête de connexion au réseau, au serveur de contrôle (CSE) via le réseau mobile (NET) en transmettant de préférence des informations spécifiques à un équipement mobile: 15 IMEISV (International Mobile Equipment Identity and Software Version Number) et un code propre à un module d'abonné: IMSI (International Mobile Subscriber Identity). Le premier numéro IMEISV est une suite de 16 chiffres contenant notamment un code d'homologation du fabricant de l'équipement mobile un numéro de série identifiant physiquement l'équipement mobile de manière unique et la 20 version de logiciel installée sur l'équipement mobile en question. Le second numéro IMSI est une suite de 15 chiffres et comprend un code attribué par l'opérateur auprès duquel un utilisateur a souscrit un abonnement permettant d'identifier un abonné de manière unique. Pour des équipements mobiles réalisés selon des normes antérieures établies par ETSI (European Telecommunications Standards 25 Institute), la combinaison du numéro IMEI composé d'une suite de 15 chiffres et du numéro SVN composé d'une suite de 2 chiffres fournit également les informations nécessaires à la réalisation de la méthode.

Lors de l'identification d'un équipement mobile, le serveur de contrôle (CSE) analyse et vérifie les données (ID) transmises en les confrontant avec le contenu 30 d'une liste noire (données à rejeter) ou d'une liste blanche (données acceptées).

- 10 -

Une base de données permet d'affiner, si nécessaire, l'identification d'un abonné et de déterminer ses particularités telles que services autorisés, paiements de l'abonnement et/ou des services effectués ou non, période d'abonnement, profil de sécurité associé à l'équipement mobile utilisé, applications installées sur  
5 l'équipement mobile, ressources disponibles sur le module de sécurité, préférences de l'utilisateur de l'équipement mobile, etc. Les résultats de cette vérification sont ensuite utilisés dans le but de déterminer un cryptogramme, appelé jeton (J), que le serveur de contrôle (CSE) transmet à l'équipement mobile (CB). Il est à noter que le serveur de contrôle (CSE) peut être distinct de l'opérateur mobile et la requête  
10 provenant d'un équipement mobile sera acheminée vers cette autorité de contrôle.

L'environnement d'exécution d'applications (AEE) de l'équipement mobile (CB) transmet le jeton (J) tel quel, sans l'altérer, au module d'abonné, l'équipement mobile (CB) jouant un rôle de relais uniquement.

Si le jeton (J) est valable, le module d'abonné peut libérer; respectivement bloquer  
15 certaines ressources (RES). La ou les applications (APP) peuvent ainsi s'exécuter selon les critères imposés par le serveur de contrôle (CSE). En effet, le jeton (J) inclut ou est accompagné d'instructions particulières à destination du module d'abonné qui peuvent conditionner le fonctionnement de l'une ou l'autre des applications (APP) de l'équipement mobile (CB). Par exemple l'exécution de  
20 transactions financières peut être limitée lorsque l'abonné se trouve être connecté à un autre réseau que celui auprès duquel il est abonné, par exemple dans un pays différent de celui de son domicile (roaming) en raison de certains critères de sécurité ou de préférences de l'abonné ou de préférences du fournisseur du service financier ou de contraintes légales en vigueur dans le pays en question. Dans un  
25 autre cas, lorsqu'un module d'abonné est inséré dans un équipement mobile (CB) non reconnu ou non homologué par l'opérateur, le jeton (J) retourné par le serveur de contrôle (CSE) peut bloquer des ressources (RES) du module d'abonné et, de ce fait empêcher ou altérer, l'exécution de ou des applications (APP).

Dans le cas d'un possible clonage de l'équipement mobile (CB) et/ou du module  
30 d'abonné (SIM), les résultats de la vérification avec la base de données comporteront des instructions dépendant des risques que l'opérateur accepte de

- 11 -

prendre avec des téléphones mobiles clonés. Par exemple, le jeton (J) généré en conséquence peut soit bloquer toutes les ressources (RES) du module d'abonné, soit limiter leur utilisation dans le temps et/ou créer un message d'avertissement à l'abonné via l'environnement d'exécution des applications (AEE).

- 5 Le jeton (J) peut être par exemple associé à une signature générée à l'aide d'une clé privée RSA, (Rivest, Shamir, Adelman)  $K_{RSA\_Pri}$  à partir d'un ensemble de données contenant, par exemple, l'IMSI, l'IMEISV, les références des ressources du module d'abonné, un compteur. Cette clé ne serait connue que du serveur de contrôle, alors que sa partie publique  $K_{RSA\_Pub}$  serait connue du module d'abonné.
- 10 L'avantage de l'utilisation de clés asymétriques réside en ce que la clé servant à créer des signatures ne se trouve pas à l'extérieur du serveur de contrôle (CSE).

Bien entendu, d'autres algorithmes à clés asymétriques tels que par exemple DSA (Digital Signature Algorithm), et ECC (Elliptic Curve Cryptography) peuvent constituer des alternatives à RSA.

- 15 L'usage d'algorithme à clés symétriques peut être préféré pour des raisons de simplicité, de rapidité des vérifications ou de coûts de fabrication et de mise en œuvre plus faibles. Dans ce cas, la clé serait connue du serveur (CSE) et du module d'abonné, par exemple un algorithme IDEA (International Data Encryption Algorithm) pourrait être utilisé pour signer l'ensemble (IMSI, IMEISV, références des ressources du module d'abonné, compteur). Comme alternative à l'algorithme IDEA, des algorithmes tels que, par exemple, TDES (Triple Data Encryption Standard) et AES (Advanced Encryption Standard) peuvent aussi être utilisés.
- 20

Dans ces deux variantes à clés asymétriques et symétriques, le module d'abonné vérifie la concordance des différents champs apparaissant dans le jeton (J),  
25 notamment elle contrôle le compteur (CPT) en le comparant avec un compteur correspondant mémorisé dans la carte qui est régulièrement maintenu à jour. Ce compteur permet d'éviter le double usage d'un même jeton (J) adressé au module d'abonné afin d'empêcher une attaque par répétition (replay attack).

Une variante au compteur est d'utiliser un aléa (nombre aléatoire) généré par le  
30 module d'abonné. Cet aléa est transmis avec les données envoyées au serveur de

- 12 -

contrôle. Ce dernier renvoie cet aléa dans le cryptogramme de réponse et le module d'abonné peut vérifier qu'il s'agit bien d'un nouveau message. Plus généralement, afin d'éviter tout risque d'usage d'un ancien cryptogramme, ce dernier comprend une variable prédictible par le module d'abonné, soit un compteur ou un aléa.

- 5 Le module d'abonné considère aussi les références des ressources (RES) dont il autorise ou non l'utilisation par les applications exécutées dans l'équipement mobile (CB).

Le module d'abonné ne connaît pas en tant que telle les références d'applications (APP) installées dans l'équipement mobile (CB). En effet, certaines applications plus 10 globales possèdent une interface relativement ouverte qui leur permet d'être utilisées par n'importe quelles applications secondaires externes. Par exemple, sur une application générale de paiement peuvent se greffer des applications particulières en fonction du mode de paiement utilisé. Le module d'abonné ne peut se baser que sur les références de ses propres ressources (RES) (données ou 15 fonctions). En acceptant les risques liés à un équipement mobile, l'opérateur fait un choix en sachant quelles ressources (RES) du module d'abonné sont utilisées par quelle(s) application(s) (APP) exécutées dans l'équipement mobile (CB).

Dans une autre variante la signature faite à l'aide d'une clé du type RSA ou IDEA peut être remplacée par un bloc généré avec une clé partagée HMAC (Keyed- 20 Hashing for Message Authentication) à partir de l'ensemble (IMSI, IMEISV, références de ressources du module d'abonné, compteur). HMAC est un mécanisme pour l'authentification de messages par l'utilisation de fonctions de hachage cryptographiques telles que MD5 (Message Digest) ou SHA-1 (Secure Hash Algorithm), en combinaison avec une clé partagée c'est-à-dire que la même clé se 25 trouve dans le serveur de contrôle (CSE) et dans le module d'abonné.

Cette clé présente à la fois dans le serveur de contrôle (CSE) et dans le module d'abonné peut être chargée lors de la personnalisation du module d'abonné ou lors de l'installation de certaines ressources dans le module d'abonné. Selon les options, à chaque ressource ou groupe de ressources du module d'abonné peut

- 13 -

être associée une clé différente, ou la clé peut être globale pour l'ensemble des ressources et unique pour un module d'abonné donné.

Pour plus de sécurité, lorsque le module d'abonné a reçu un jeton (J), il peut retransmettre au serveur de contrôle (CSE), via l'équipement mobile (CB) et le 5 réseau mobile (NET), un message de confirmation (CF) attestant la bonne réception et le traitement adéquat du jeton (J) par le module d'abonné. La confirmation (CF) comprend au moins un code de succès ou d'erreur de l'opération ainsi qu'un compteur, similaire à celui du jeton (J), servant à la protection contre les attaques par répétition. Ce message permet aussi au serveur de contrôle (CSE) de tenir à 10 jour le compteur associé au module d'abonné.

Dans une variante de l'invention, l'équipement mobile peut être remplacé par un équipement non mobile tel qu'un décodeur de télévision à péage ou un ordinateur. Le serveur de contrôle reçoit de la part d'un module de sécurité, l'équivalent du 15 module d'abonné, l'identifiant de l'équipement connecté au réseau et l'identifiant du module de sécurité. En réponse, le serveur effectue les vérifications telles que décrites plus haut et renvoie un cryptogramme au module de sécurité. Cette réponse va libérer ou bloquer des ressources dans le module de sécurité.

## REVENDICATIONS

1. Méthode de gestion de la sécurité d'applications (APP) fonctionnant dans un équipement (CB) connecté à un réseau (NET), ledit réseau (NET) étant administré par un serveur de contrôle (CSE) d'un opérateur, lesdites applications utilisant des ressources (RES) (données ou fonctions) stockées dans un module de sécurité (SIM) relié localement audit équipement (CB), comprenant les étapes préliminaires suivantes:

- réception de données comprenant au moins le type et la version de logiciel de l'équipement (CB) et l'identité du module de sécurité (SIM), via le réseau, par le serveur de contrôle,
- analyse et vérification par le serveur de contrôle (CSE) desdites données (ID),
- génération d'un cryptogramme (J) à partir du résultat de la vérification sur lesdites données (ID), et transmission dudit cryptogramme (J), via le réseau (NET) et l'équipement (CB), au module de sécurité (SIM),

ladite méthode est caractérisée en ce que le module de sécurité (SIM) analyse le cryptogramme (J) reçu et active, respectivement désactive des ressources (RES) (données ou fonctions) utilisées par au moins une application (APP) installée dans l'équipement (CB), ledit cryptogramme (J) comprenant des instructions conditionnant le fonctionnement de l'application (APP) selon des critères établis par le fournisseur de ladite application et/ou l'opérateur et/ou l'utilisateur de l'équipement.

2. Méthode selon la revendication 1, caractérisée en ce que l'équipement (CB) est un équipement mobile de téléphonie mobile.

3. Méthode selon la revendication 1, caractérisée en ce que le réseau est un réseau mobile du type GSM, GPRS ou UMTS.

4. Méthode selon les revendications 1 et 2, caractérisée en ce que le module de sécurité (SIM) est un module d'abonné inséré dans l'équipement mobile de téléphonie mobile de type carte SIM.

5. Méthode selon les revendications 1 à 4, caractérisée en ce que l'identification de l'ensemble équipement mobile / module d'abonné (SIM) est effectuée à partir de

- 15 -

l'identifiant (IMEISV) de l'équipement mobile (CB) et du numéro d'identification du module d'abonné (IMSI) propre à un abonné au réseau mobile.

6. Méthode selon la revendication 1 à 5, caractérisée en ce que les critères définissent des limites d'utilisation d'une application (APP) selon des risques associés ladite application (APP) et au type et la version de logiciel de l'équipement mobile que l'opérateur et/ou le fournisseur d'applications et/ou l'utilisateur de l'équipement mobile désirent prendre en compte.

7. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute après chaque connexion de l'équipement mobile au réseau.

8. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute après chaque mise à jour de la version de logiciel de l'équipement mobile.

9. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute après chaque activation ou désactivation d'une application sur l'équipement mobile.

10. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute après chaque mise à jour de la version de logiciel du module d'abonné.

11. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute après chaque mise à jour de ressources sur le module d'abonné.

12. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute périodiquement à un rythme donné par le serveur de contrôle.

13. Méthode selon les revendications 1 à 6, caractérisée en ce qu'elle s'exécute après chaque démarrage d'une application sur l'équipement mobile.

14. Méthode selon l'une des revendications précédentes, caractérisée en ce que le module d'abonné (SIM), préalablement à l'exécution des instructions données par le cryptogramme (J), compare l'identifiant (IMEISV) de l'équipement mobile (CB) avec celui précédemment reçu et initie l'opération de vérification seulement si l'identifiant (IMEISV) a changé.

- 16 -

15. Méthode selon les revendications 1 à 5, caractérisée en ce que le serveur de contrôle (CSE), préalablement à la transmission du cryptogramme (J), compare l'identifiant (IMEISV) de l'équipement mobile avec celui précédemment reçu et initie l'opération de vérification seulement si l'identifiant (IMEISV) a changé.

16. Méthode selon les revendications 1 à 15, caractérisée en ce que le cryptogramme (J) est constitué par un message encrypté par le serveur de contrôle (CSE) à l'aide d'une clé d'encryption asymétrique ou symétrique à partir d'un ensemble de données contenant, entre autres données, l'identifiant (IMEISV) de l'équipement mobile (CB), le numéro d'identification du module d'abonné (IMSI), des références de ressources (RES) du module d'abonné (SIM) et une variable prédictible (CPT).

17. Méthode selon les revendications 1 à 16 caractérisée en ce que le module d'abonné transmet au serveur de contrôle (CSE), via l'équipement mobile (CB) et le réseau mobile (NET), un message de confirmation (CF) lorsque le module abonné (SIM) a reçu le cryptogramme (J), ledit message attestant la bonne réception et le traitement adéquat du cryptogramme (J) par le module d'abonné (SIM).

18. Méthode selon la revendication 1, caractérisée en ce que l'équipement est un décodeur de télévision à péage ou un ordinateur auquel est connecté le module de sécurité.

19. Module de sécurité comprenant des ressources (RES) destinées à être localement accédées par au moins une application (APP) installée dans un équipement (CB) relié à un réseau (NET), ledit équipement comprenant des moyens de lecture et de transmission de données comprenant au moins l'identifiant (IMEISV) de l'équipement et l'identifiant (IMSI) du module de sécurité, ledit module étant caractérisé en ce qu'il comprend des moyens de réception, d'analyse et d'exécution d'instructions contenues dans un cryptogramme (J), lesdites instructions conditionnant le fonctionnement de l'application (APP) selon des critères préétablis par le fournisseur de ladite application (APP) et/ou l'opérateur) et/ou l'utilisateur de l'équipement (CB).

- 17 -

20. Module de sécurité selon la revendication 19, caractérisé en ce qu'il constitue un module d'abonné du type "carte SIM" connecté à un équipement mobile.

1/1

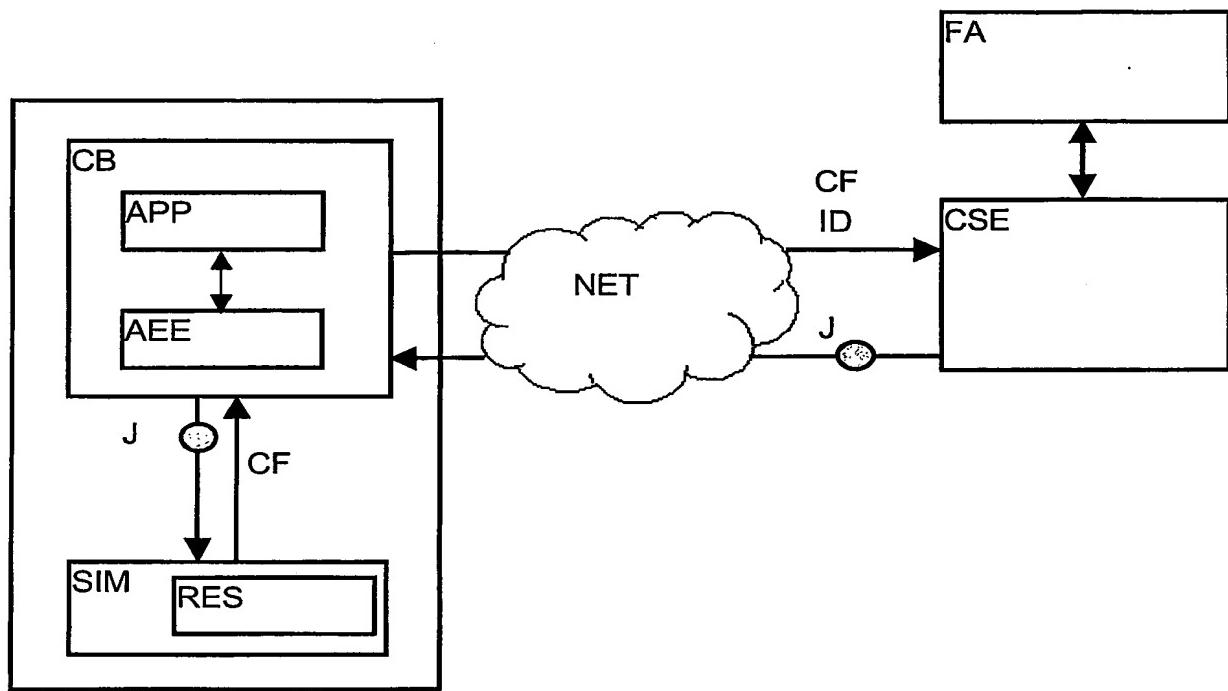


Fig.1

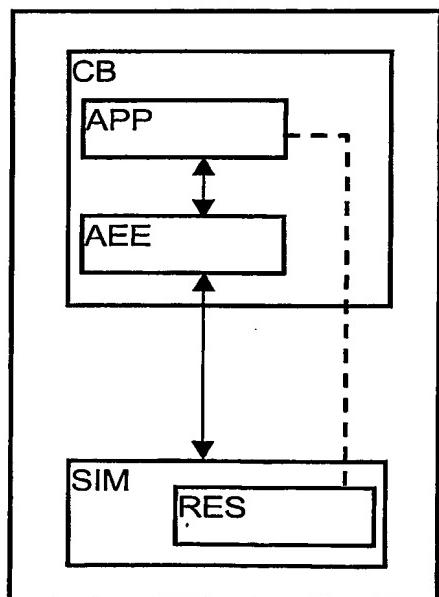


Fig. 2